AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1.   (Currently amended) A method ~~of determining a packet signature in a router~~, comprising:

computing a signature of the router's network address;

receiving a packet at the router;

zeroing out selected fields in the received packet; ~~and~~

computing a signature of the received packet using the computed signature of the router's network address; and

<u>using the signature in determining a point of ingress for the packet when it entered a network.</u>

2.   (Original) The method of claim 1, wherein the selected fields comprise at least one of a time-to-live field, a type-of-service field, and a checksum field.

3.   (Original) The method of claim 1, wherein the signatures comprise cyclic redundancy checking (CRC) values.

4.   (Original) The method of claim 3, wherein the CRC values comprise CRC-32 values.

5.   (Original) The method of claim 1, wherein the signatures comprise hash values.

6.   (Currently amended) A method ~~of archiving signatures associated with packets received at nodes in a network~~, comprising:

receiving packets at a plurality of the nodes in ~~the~~ <u>a</u> network;

computing first signatures of the network addresses of each of the plurality of nodes; computing one or more second signatures for each of the received packets using the computed first signatures; ~~and~~

archiving the one or more computed second signatures in a memory device<u>; and</u>

<u>providing the archived one or more computed second signatures to an agent for tracing a path that a given packet traversed in a network</u>.

7.   (Original) The method of claim 6, wherein computing the one or more second signatures for each of the received packets further comprises:

computing one or more cyclical redundancy checking values for each of the received packets.

8.   (Original) The method of claim 6, wherein computing the one or more second signatures of each of the received packets further comprises:

computing one or more hash values for each of the received packets.

9.   (Original) The method of claim 6, wherein computing the one or more second signatures of each of the received packets further comprises:

computing one or more CRC-32 values for each of the received packets.

10.   (Currently amended) A method ~~of archiving signatures associated with packets~~

~~received at a node in a network~~, comprising:

        receiving packets at the node;

        computing one or more signatures for each of the received packets;

        aggregating the computed one or more signatures in a first memory to produce

one or more signature vectors; ~~and~~

        archiving the one or more signature vectors in a second memory; and

        providing the archived one or more signature vectors to an agent for determining a

point of ingress for the packet when it entered a network.

11.   (Original) The method of claim 10, wherein computing the one or more signatures

for each of the received packets further comprises:

        computing one or more cyclical redundancy checking values for each of the

received packets.

12.   (Original) The method of claim 10, wherein computing the one or more signatures

for each of the received packets further comprises:

        computing one or more hash values for each of the received packets.

13.   (Original) The method of claim 10, wherein computing the one or more signatures

for each of the received packets further comprises:

computing one or more CRC-32 values for each of the received packets.

14.   (Original) The method of claim 10, wherein the second memory comprises a ring buffer.

15.   (Original) The method of claim 10, wherein the computed one or more signatures are aggregated over a collection interval R.

16.   (Original) The method of claim 15, wherein archiving the one or more signature vectors comprises:

        storing the one or more signature vectors in the second memory indexed by the collection interval.

17.   (Original) The method of claim 10, wherein archiving the one or more signature vectors comprises:

storing a fraction of the one or more signature vectors in the second memory.

18.   (Original) The method of claim 10, further comprising:

discarding signature vectors of the archived one or more signature vectors that are older than P seconds.

19.   (Original) The method of claim 15, further comprising:

randomly zeroing out a fraction of the one or more signature vectors that are older

than P seconds.

20.   (Original) The method of claim 19, further comprising:

merging bits of the signature vectors that are older than P seconds.

21.   (Original) The method of claim 20, further comprising:

archiving the merged bits in the second memory for a period equaling a multiple

of the collection interval R.

22.   (Original) The method of claim 21, wherein the multiple of the collection interval

R comprises 10*R.

23.   (Original) The method of claim 10, wherein the second memory comprises a

DRAM.

24.   (Original) An apparatus for archiving signatures associated with packets received

at a node in a network, comprising:

a first memory;

a second memory;

a signature tap configured to:

receive packets at the node;

compute one or more signatures for each of the received packets;

a multiplexer configured to:

aggregate the computed one or more signatures in the first memory to

produce one or more signature vectors; and

a controller configured to:

archive the one or more signature vectors in the second memory.

25.   (Original) The apparatus of claim 24, the one or more signature vectors

comprising one or more cyclical redundancy checking values.

26.   (Original) The apparatus of claim 24, the one or more signature vectors

comprising one or more hash values.

27.   (Original) The apparatus of claim 24, the one or more signature vectors

comprising one or more CRC-32 values.

28.   (Original) The apparatus of claim 24, wherein the second memory comprises a

ring buffer.

29.   (Original) The apparatus of claim 24, the multiplexer further configured to:

aggregate the one or more signatures over a collection interval R.

30.   (Original) The apparatus of claim 29, the controller further configured to:

store the one or more signature vectors in the second memory indexed by the

collection interval.

31.   (Original) The apparatus of claim 24, the controller further configured to:

store a fraction of the one or more signature vectors in the second memory.

32.   (Original) The apparatus of claim 24, the controller further configured to:

discard signature vectors of the archived one or more signature vectors that are

older than P seconds.

33.   (Original) The apparatus of claim 29, the controller further configured to:

randomly zero out a fraction of the one or more signature vectors that are older

than P seconds.

34.   (Original) The apparatus of claim 33, the controller further configured to:

merge bits of the signature vectors that are older than the P seconds.

35.   (Original) The apparatus of claim 34, the controller further configured to:

archive the merged bits in the second memory for a period equaling a multiple of

the collection interval R.

36.   (Original) The apparatus of claim 35, wherein the multiple of the collection

interval R comprises 10*R.

37.   (Original) The apparatus of claim 24, wherein the second memory comprises a

DRAM.

38.   (Canceled)

39.   (New) A system, comprising:

a first memory;

a second memory;

one or more signature taps configured to:

        receive packets at the node, and

        compute one or more signatures for each of the received packets;

a multiplexer configured to:

        use each of the one or more signatures as addresses for addressing bit

locations in the first memory,

        set memory bits in the addresses of the first memory corresponding to

each of the one or more signatures; and

a controller configured to archive a signature vector comprising a block of

memory bits from the first memory in the second memory.

40.   (New) A system, comprising:

a first memory;

a second memory;

a signature tap to determine at least one signature for each packet of a plurality of

received packets;

a multiplexer to store, over a collection interval, the determined at least one

signature packet for each of the plurality of received packets in the first memory to

produce a signature vector that comprises a block of a plurality of signatures for at least a

portion of the plurality of received packets; and

a controller configured to archive the one or more signature vectors in the second

memory after an expiration of the collection interval.